巡回符号の分解 (実験配置の組合せ数学と群論)

AUTHOR(S):

嵩, 忠雄

CITATION:

嵩, 忠雄. 巡回符号の分解 (実験配置の組合せ数学と群論). 数理解析研究所講究録 1974, 211: 40-46

ISSUE DATE:

1974-06

URL:

http://hdl.handle.net/2433/105211

数理解析研究所講究録
211巻 1974年 40-46

巡回符号の分解

阪大 基礎工 嵩 忠雄

§1. 巡回符号の漸近的性質

$H(x) = -x\log_2 x - (1-x)\log_2(1-x)$とする．正整数$r$，$d$（ただし，$r > d$）が与えられたとき，

$$\frac{r}{n} \leq H\left(\frac{d}{n}\right) \qquad (1)$$

を満すnについて，符号長n，検査点数rで最小重みがd以上の2元線形符号が存在する（Gilbert-Varshamov下界式[1,2]）．

組織符号の無限の系列C_1，C_2，… があって$0 < R < 1$，$0 < \delta < 1$について，つぎの条件を満すとき，この系列を漸近的によいという．

$$n_i < n_{i+1},$$
$$R \leq k_i / n_i,$$
$$\delta \leq d_i / n_i,$$

ここで，n_i，k_i，d_i，はそれぞれC_iの符号長，情報点数最

小重みである．(1) より $H(\delta) \leq 1-R$ を満す δ，R について漸近的によい2元線形符号の系列が存在する．さらに，Goppa 符号や，[3] 既約多項式を生成多項式とする短縮巡回符号についても同様のことが成立する．[4] ところが，漸近的によい巡回符号の系列が存在するかどうか知られていない．

符号長が $2k$，情報点数が k の2元線形符号で，ベクトルの第 i 成分を第 $i+2 \pmod{2k}$ 成分へシフトする置換で不変に保たれるものを2-擬巡回符号という．[1]

$$\frac{10,006,699}{10,006,698} H(\delta) \leq \frac{1}{2} \qquad (2)$$

を満す δ と $R = 1/2$ について，漸近的によい2-擬巡回符号の系列が存在する．[5] 奇数 a について，$a \mid 2^m - 1$ を満す2以上の最小整数 m を $M(a)$ とかくと，(2) の左辺の係数は，$M(p) = p-1$，$M(p) < M(p^2)$ を満す任意の奇素数 p をとり，$p/(p-1)$ でおきかえることができる．

符号長 n の2元線形符号 C に対して，$C_{ex} = \{(\sum_{i=1}^{n} v_i, v_1, \cdots, v_n) \mid (v_1, v_2, \cdots, v_n) \in C\}$ を C の拡大符号という．

$n = 2^m - 1$ のとき，α を $GF(2^m)$ の原始元とし，ベクトルの第1，第2，第3，$\cdots$，第 2^m 成分に，$0, \alpha^0, \alpha^1, \cdots, \alpha^{2^m-2}$ を対応させる．任意の $A \neq 0$，$B \in GF(2^m)$ について，変換 $X \leftarrow AX + B$ でひきおこされる成分位置の置換により C_{ex}

が不変に保たれるとき，Cをアフィン不変であるという.[1] BCH符号はじめ多くの主要な符号はアフィン不変である．漸近的によいアフィン不変な符号の系列は存在しないことが証明されている.[4] とくに，符号長が$n=2^m-1$の形のBCH符号について，$m\to\infty$のとき

$$\frac{d}{n}\sim\frac{2\ln(n/k)}{m} \tag{3}$$

が成立する.[6] 巡回符号のいくつかのクラスについて，d/nの下界式として知られているなかで，nが十分大きいとき，最良の形は$f(n/k)/\log_2 n$である．最近，巡回連接符号のあるクラスについて，もし，

$$M(p)=(p-1)/2 \tag{4}$$

を満す素数が無限に存在するならば，$K/n\approx$定数で，

$$\frac{d}{n}\geq\left(1-\frac{2k}{n}\right)\frac{1}{\sqrt{2\log_2 n}} \tag{5}$$

を満す巡回符号の無限の系列が存在することが示された.[7]
次節で巡回連接符号の拡張とそれに関連した二，三の問題について述べる．

§2．巡回符号の合成と分解

φをある素数のべキ乗とし，n_0をφと互に素な正整数と

する．C_0 を q 元の (n_0, K_0) 巡回符号* とし，その検査多項式が $\xi_1(x)\xi_2(x)\cdots\xi_\ell(x)$ であるとする．ここで，$\xi_1(x)$, …, $\xi_\ell(x)$ は相異なる $GF(q)$ の上の既約多項式である．$\xi_i(x)$ の次数を r_i，$\xi_i(x)\xi_{i+1}(x)\cdots\xi_\ell(x)$ を検査多項式とする C_0 の部分符号の最小重みを d_{0i} と書く．n を n_0 と互に素な正整数とし，β，γ をそれぞれ $GF(q)$ の拡大体に属する位数 n_0, n の元とする．$\xi_i(\beta^{\nu_i})=0$ とすると，C_0 の Mattson - Solomon 多項式は[1,2] つぎのように表わされる．

$$\sum_{i=1}^{\ell} T_{q,r_i}(c_i Y^{-\nu_i}) \qquad (6)$$

ここで，$c_i \in GF(q^{r_i})$，Y の指数は $\bmod n_0$ で考え，$T_{q,r}(x) = x + x^q + \cdots + x^{q^{r-1}}$．一般に巡回符号 C の Mattson - Solomon 多項式全体の集合を $MS(C)$ と書く．よく知られているように[1,2]，α を符号長 n を位数とする $GF(q)$ の拡大体の元とするとき，

$$C = \{(\phi(\alpha^0), \phi(\alpha^1), \cdots, \phi(\alpha^{n-1})) \mid \phi \in MS(C)\} \qquad (7)$$

が成立する．

$1 \le i \le \ell$ の各 i について，C_i を q^{r_i} 元 (n, k_i) 巡回符号とし，その最小重みを d_i，その検査多項式の根を

$$\gamma^{\mu_{i1}}, \gamma^{\mu_{i2}}, \cdots, \gamma^{\mu_{ik_i}}$$

---

* 符号長 n_0，情報点数 K_0 の符号．

とする．さらに，つぎのように定義する．

$$F(C_0; C_1, C_2, \cdots, C_\ell) = \left\{ \sum_{i=1}^{\ell} T_{q,r_i}(\phi_i(Z) Y^{-\nu_i}) \mid \phi_i \in MS(C_i) \right\}$$

$f(Y, Z) \in F(C_0; C_1, C_2, \cdots, C_\ell)$ に対して，

$$\nu(f) = (f_0, f_1, \cdots, f_{nn_0-1}),$$

ここで，$f_{I(\nu,\mu)} = f(\beta^\nu, \gamma^\mu)$，$I(\nu, \mu)$ は $i \equiv \nu \pmod{n_0}$，$i \equiv \mu \pmod{n}$，$0 \le i < nn_0$ を満す整数．

$$C_0 \times (C_1, C_2, \cdots, C_\ell) = \left\{ \nu(f) \mid f(Y,Z) \in F(C_0; C_1, C_2, \cdots, C_\ell) \right\}$$

このとき，[8]

（P1） $C_0 \times (C_1, C_2, \cdots, C_\ell)$ は q 元 $(nn_0, \sum_{i=1}^{\ell} r_i k_i)$ 巡回符号であり，その最小重みは少くとも $\min_{1 \le i \le \ell} d_{0i} d_i$，検査多項式の根の集合は

$$\{ \beta^{\nu_i} \delta^s \gamma^{\mu_{ij}} \delta^s \mid 1 \le i \le \ell,\ 0 \le s < r_i,\ 1 \le j \le k_i \}$$

である．

（P2） $C_0 \times (C_1, C_2, \cdots, C_\ell)$ が巡回連接符号*であるための必要十分条件は，$C_1, C_2, \cdots, C_\ell$ が同一の生成多項式をもつことである．

巡回連接符号のいくつかのクラスについて，適当な n/K の範囲に関して，BCH符号の漸近式 (3) より若干よい漸近

---

* 連接符号の定義は文献 (1), (2)，あるいは (9) 参照．

式をもつものが知られている.[7,8] いづれも $f(n/k)/\log_2 n$ の形である.

さらに，つぎの意味で（P1）の逆が成立する.

（P3） n, n_0, q を互に素とする. C を符号長 nn_0 の q 元巡回符号とする. このとき，正整数 l, r_i $(1 \leq i \leq l)$, 符号長 n_0 の q 元巡回符号 C_0, 符号長 n の q^{r_i} 元巡回符号 C_i $(1 \leq i \leq l)$ が存在して，

$$C = C_0 \times (C_1, C_2, \cdots, C_l)$$

n を素因数に分解して，$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ とする. 符号長 n の q 元巡回符号は，符号長 $p_i^{m_i}$ の $GF(q)$ あるいはその拡大体の上の巡回符号から，(8)の構成法をくり返して得られる. このことは，巡回符号の分類や，復号法などに利用できよう.

参考文献

(1) W. W. Peterson and E. J. Weldon, Jr., "Error-Correcting Codes, 2nd Edition," Cambridge, Mass. : M.I.T. Press, 1972.

(2) E. R. Berlekamp, "Algebraic Coding Theory," New York : McGraw-Hill, 1968.

(3) V. D. Goppa, "Rational representation of codes and (L,g) codes,"

Probl. Peredach. Inform., vol. 7, pp.41-49, 1971.

(4) T. Kasami, "An upper bound on k/n for affine-invariant codes with fixed d/n," IEEE Trans. on Information Theory, IT-15, pp.174-176, 1969.

(5) T. Kasami, "Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2," to appear in IEEE Trans. on Information Theory.

(6) E. R. Berlekamp, "Long primitive binary BCH codes have distance d $\sim$ 2n ℓn R^{-1}/log n," IEEE Trans. on Information Theory, IT-18, pp.415-426, 1972.

(7) E. R. Berlekamp and J. Justesen, "Some long cyclic linear binary codes are not so bad," to appear in IEEE Trans. on Information Theory.

(8) T. Kasami, "Construction and decomposition of cyclic codes of composite length," to appear in IEEE Trans. on Information Theory.

(9) G. D. Forney, Jr., "Concatenated Codes," Cambridge, Mass. M.I.T. Press, 1966.